1. Record Nr. UNINA9910860873803321

Autore	Oppliger Rolf
Titolo	SSL and TLS : : theory and practice / / Rolf Oppliger
Pubbl/distr/stampa	Norwood : , : Artech House, , [2023] ©2023
ISBN	1-68569-016-5
Edizione	[3rd ed.]
Descrizione fisica	1 online resource (xxv, 352 pages) : illustrations
Collana	Artech House information security and privacy series
Soggetti	Computer networks - Security measures World Wide Web - Security measures Computer network protocols
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	SSL and TLS: Theory and Practice Third Edition -- Contents -- Foreword -- Preface -- References -- Acknowledgments -- Chapter 1 Introduction -- 1.1 INFORMATION AND NETWORK SECURITY -- 1.1.1 Security Services -- 1.1.2 Security Mechanisms -- 1.2 TRANSPORT LAYER SECURITY -- 1.3 FINAL REMARKS -- References -- Chapter 2 SSL Protocol -- 2.1 INTRODUCTION -- 2.2 PROTOCOLS -- 2.2.1 SSL Record Protocol -- 2.2.2 SSL Handshake Protocol -- 2.2.3 SSL Change Cipher Spec Protocol -- 2.2.4 SSL Alert Protocol -- 2.2.5 SSL Application Data Protocol -- 2.3 PROTOCOL TRANSCRIPT -- 2.4 SECURITY ANALYSIS -- 2.5 FINAL REMARKS -- References -- Chapter 3 TLS Protocol -- 3.1 INTRODUCTION -- 3.1.1 TLS PRF -- 3.1.2 Generation of Keying Material -- 3.2 TLS 1.0 -- 3.2.1 Cipher Suites -- 3.2.2 Certificate Management -- 3.2.3 Alert Messages -- 3.2.4 Other Differences -- 3.3 TLS 1.1 -- 3.3.1 Cipher Suites -- 3.3.2 Certificate Management -- 3.3.3 Alert Messages -- 3.3.4 Other Differences -- 3.4 TLS 1.2 -- 3.4.1 TLS Extensions -- 3.4.2 Cipher Suites -- 3.4.3 Certificate Management -- 3.4.4 Alert Messages -- 3.4.5 Other Differences -- 3.5 TLS 1 -- 3.5.1 Handshake Protocol -- 3.5.2 Key Derivation -- 3.5.3 Certificate Management -- 3.5.4 Alert Messages -- 3.5.5 Other Differences -- 3.6 HSTS -- 3.7 PROTOCOL TRANSCRIPTS -- 3.7.1 TLS 1.0 -- 3.7.2 TLS 1.2 -- 3.8 SECURITY ANALYSIS -- 3.9 FINAL REMARKS -- References --

Chapter 4 DTLS Protocol -- 4.1 INTRODUCTION -- 4.2 DTLS 1.0 -- 4.2.1 Record Protocol -- 4.2.2 Handshake Protocol -- 4.3 DTLS 1.2 -- 4.4 DTLS 1.3 -- 4.4.1 Record Protocol -- 4.4.2 Handshake Protocol -- 4.5 SECURITY ANALYSIS -- 4.6 FINAL REMARKS -- References -- Chapter 5 Firewall Traversal -- 5.1 INTRODUCTION -- 5.2 SSL/TLS TUNNELING -- 5.3 SSL/TLS PROXYING -- 5.4 MIDDLEBOX MITIGATION -- 5.5 FINAL REMARKS -- References -- Chapter 6 Public Key Certificates and Internet PKI.
6.1 INTRODUCTION -- 6.2 X.509 CERTIFICATES -- 6.2.1 Certificate Format -- 6.2.2 Hierarchical Trust Model -- 6.3 SERVER CERTIFICATES -- 6.4 CLIENT CERTIFICATES -- 6.5 PROBLEMS AND PITFALLS -- 6.6 CERTIFICATE LEGITIMATION -- 6.6.1 Public Key Pinning -- 6.6.2 DNS Resource Records -- 6.6.3 Distributed Notaries -- 6.6.4 Certificate Transparency -- 6.7 FINAL REMARKS -- References -- Chapter 7 Concluding Remarks -- References -- Appendix A Attacks Against SSL/TLS -- A.1 BLEICHENBACHER ATTACK -- A.1.1 DROWN, ROBOT, and CATs -- A.1.2 Kl´ma-Pokorn´y-Rosa Attack -- A.1.3 Manger Attack -- A.2 VAUDENAY ATTACK -- A.3 BEAST -- A.4 POODLE -- A.5 RENEGOTIATION ATTACKS -- A.6 COMPRESSION-RELATED ATTACKS -- A.7 KEY EXCHANGE DOWNGRADE ATTACKS -- A.7.1 FREAK -- A.7.2 Logjam -- References -- Appendix B TLS Cipher Suites -- Reference -- Appendix C TLS Extensions -- C.1 OVERVIEW -- C.2 DETAILED EXPLANATIONS -- C.2.1 Server name (0) Extension -- C.2.2 Max fragment length (1) and Record size limit (28) Extensions -- C.2.3 Client certificate url (2) Extension -- C.2.4 Trusted ca keys (3) Extension -- C.2.5 Truncated hmac (4) Extension -- C.2.6 Status request (5) and Status request v2 (17) Extensions -- C.2.7 User mapping (6) Extension -- C.2.8 Client authz (7) and Server authz (8) Extensions -- C.2.9 Cert type (9) Extension -- C.2.10 Supported groups (10) and ec point formats (11) Extensions -- C.2.11 Srp (12) Extension -- C.2.12 Signature algorithms (13) Extension -- C.2.13 Use srtp (14) Extension -- C.2.14 Heartbeat (15) Extension -- C.2.15 Application layer protocol negotiation (16) Extension -- C.2.16 Signed certificate timestamp (18) and transparency info (52) Extensions -- C. 2.17 Client certificate type (19) and Server certificate_type (20) Extensions -- C.2.18 Padding (21) Extension -- C.2.19 Encrypt then mac (22) Extension -- C.2.20 Token binding (24) Extension.
C.2.21 Cached info (25) Extension -- C.2.22 Compress certificate (27) Extension -- C.2.23 Pwd protect (29), pwd clear (30), and password salt (31) Extensions -- C.2.24 Ticket pinning (32) Extension -- C.2.25 Tls cert with extern psk (33) Extension -- C.2.26 Session ticket (35) and ticket request (58) Extension -- C.2.27 TLMSP (36), TLMSP proxying (37), and TLMSP delegate (38) Extensions -- C.2.28 Supported ekt ciphers (39) Extension -- C.2.29 Pre shared key (41) Extension -- C. 2.30 Early data (42) Extension -- C.2.31 Supported versions (43) Extension -- C.2.32 Cookie (44) Extension -- C.2.33 Psk key exchange modes (45) Extension -- C.2.34 Certificate authorities (47) Extension -- C.2.35 Oid filters (48) Extension -- C.2.36 Post handshake auth (49) Extension -- C.2.37 Signature algorithms cert (50) Extension -- C.2.38 Key share (51) Extension -- C.2.39 Connection id (54) Extension -- C. 2.40 External id hash (55) and external session id (56) Extensions -- C. 2.41 Quic transport parameters (57) Extention -- C.2.42 Dnssec chain (59) Extension -- C.2.43 Renegotiation info (65281) and extended master secret (23) Extensions -- References -- Abbreviations and Acronyms -- About the Author -- Index.

Sommario/riassunto

Now in its Third Edition, this completely revised and updated reference provides a thorough and comprehensive introduction into the SSL, TLS, and DTLS protocols, explaining all the details and technical subtleties

and showing how the current design helps mitigate the attacks that have made press headlines in the past. The book tells the complete story of TLS, from its earliest incarnation (SSL 1.0 in 1994), all the way up to and including TLS 1.3. Detailed descriptions of each protocol version give you a full understanding of why the protocol looked like it did, and why it now looks like it does. You will get a clear, detailed introduction to TLS 1.3 and understand the broader context of how TLS works with firewall and network middleboxes, as well the key topic of public infrastructures and their role in securing TLS. You will also find similar details on DTLS, a close sibling of TLS that is designed to operate over UDP instead of TCP. The book helps you fully understand the rationale behind the design of the SSL, TLS, and DTLS protocols and all of its extensions. It also gives you an in-depth and accessible breakdown of the many vulnerabilities in earlier versions of TLS, thereby more fully equipping you to properly configure and use the protocols in the field and protect against specific (network-based) attacks. With its thorough discussion of widely deployed network security technology, coupled with its practical applications you can utilize today, this is a must-have book for network security practitioners and software/web application developers at all levels.